

①⑨ RÉPUBLIQUE FRANÇAISE  
INSTITUT NATIONAL  
DE LA PROPRIÉTÉ INDUSTRIELLE  
PARIS

①⑪ N° de publication : **2 770 067**  
(à n'utiliser que pour les  
commandes de reproduction)

②① N° d'enregistrement national : **97 12973**

⑤① Int Cl<sup>6</sup> : H 04 L 9/12, G 06 F 12/14 // G 07 F 7/10

①⑫

## DEMANDE DE BREVET D'INVENTION

A1

②② Date de dépôt : 16.10.97.

③① Priorité :

④③ Date de mise à la disposition du public de la  
demande : 23.04.99 Bulletin 99/16.

⑤⑥ Liste des documents cités dans le rapport de  
recherche préliminaire : *Se reporter à la fin du  
présent fascicule*

⑥① Références à d'autres documents nationaux  
apparentés :

⑦① Demandeur(s) : FRANCE TELECOM SOCIETE ANO-  
NYME — FR.

⑦② Inventeur(s) : MOUNIER JEAN PIERRE.

⑦③ Titulaire(s) :

⑦④ Mandataire(s) : SOCIETE DE PROTECTION DES  
INVENTIONS.

⑤④ PROCEDE D'ACCES A UNE APPLICATION.

⑤⑦ La présente invention concerne un procédé d'accès à  
une application dans lequel on utilise un code confidentiel.  
Dans ce procédé on prévoit en accord avec l'usager du co-  
de, un algorithme d'évolution de ce code en partant d'un  
code de base.

FR 2 770 067 - A1



BEST AVAILABLE COPY

PROCEDE D'ACCES A UNE APPLICATIONDESCRIPTION5 Domaine technique

La présente invention concerne un procédé d'accès à une application, dans lequel on utilise un code confidentiel.

10

Etat de la technique antérieur

L'accès à de nombreuses applications est protégé par l'utilisation d'un code confidentiel. Ce  
15 code peut être modifié par l'intéressé, pour un accès à son calculateur personnel par exemple, ou par les responsables de ces applications.

Si quelqu'un prend connaissance du code personnel donnant accès à une application (vol d'une  
20 carte avec le code par exemple) il lui est aisé de s'introduire frauduleusement dans l'application. Il lui est aussi possible de faire des essais multiples de codes d'accès. Pour résoudre ce problème il est possible de changer un code et de le mémoriser, mais  
25 cette procédure est lourde.

L'invention a pour objet de changer automatiquement le code, autant de fois qu'on le veut, en possédant un moyen simple de s'en souvenir.

30

Exposé de l'invention

La présente invention concerne un procédé d'accès à une application dans lequel on utilise un  
35 code confidentiel, caractérisé en ce qu'on prévoit, en

accord avec l'utilisateur du code, un algorithme d'évolution du code en partant d'un code de base.

Avantageusement l'algorithme est pris parmi les algorithmes suivants :

- 5                   - algorithmes utilisant l'heure ;
- algorithmes utilisant le jour de la semaine ;
- algorithmes utilisant la semaine ;
- algorithmes utilisant le jour du mois ;
- 10                  - algorithmes utilisant le mois ;
- algorithmes utilisant l'année ;
- algorithmes utilisant une table particulière ;
- algorithmes utilisant plusieurs
- 15 paramètres, qui sont la concaténation de plusieurs algorithmes.

On peut de plus utiliser un algorithme de secours.

- Avantageusement la modification
- 20 d'algorithme peut être faite en ligne ou via un mécanisme de changement automatique connu à la fois par le propriétaire du code et le serveur associé à l'application que l'on veut utiliser.

- Le mécanisme peut être introduit dans toute
- 25 application qui demande un code d'accès.

- Toutes les applications informatiques peuvent utiliser ce type de codes pour se protéger. On peut, par exemple, s'en servir pour contrôler un code d'accès et autoriser ou non un accès à certaines
- 30 heures.

Dans un exemple de réalisation l'utilisateur utilise une carte. On peut alors avoir les étapes suivantes :

- à l'achat d'une carte, l'utilisateur choisit,
- 35 dans un catalogue, l'algorithme qu'il désire et donne

les paramètres qui seront utilisés par cet algorithme ;  
le vendeur de la carte saisit le numéro de l'algorithme  
et les paramètres ; le serveur remplit la table  
correspondant au fichier de l'utilisateur ;

5                   - quand l'utilisateur introduit sa carte, les  
caractéristiques de la carte et du terminal permettent  
de :

- identifier le porteur de la carte et de  
trouver son fichier,
- 10           • savoir s'il a accès à l'application et  
s'il peut l'utiliser actuellement,
- connaître sa table de code ;
- l'utilisateur frappe le code correspondant aux  
paramètres qu'il a lui-même définis.

15

#### Brève description des figures

- La figure illustre le contexte  
d'utilisation du procédé de l'invention.

20

#### Exposé détaillé de modes de réalisation

L'invention consiste à prévoir, en accord  
avec l'utilisateur du code, un algorithme d'évolution de  
25 celui-ci en partant d'un code de base, cette évolution  
pouvant avoir lieu n'importe quand, avec n'importe  
quelle fréquence.

Dans un premier exemple : sur le code JPM  
on décide de greffer l'heure et le jour sous la forme  
30 J14P11M où 14 représente l'heure (2 pm) et onze mois.  
Au pire il peut y avoir une incertitude à la frontière  
de l'heure mais on peut présenter deux codes  
successivement.

Dans un second et un troisième exemples :  
 au code CESTMOI on peut ajouter le jour de la semaine  
 codé ou éliminer une lettre :

5	le dimanche	CESTMOIREPOS	ou	ESTMOI
	le lundi	CESTMOIDEBUT	ou	CSTMOI
	le mardi	CESTMOIMARS	ou	CETMOI
	le mercredi	CESTMOIECOL	ou	CESMOI
	le jeudi	CESTMOIJEUD	ou	CESTOI
10	le vendredi	CESTMOIFINI	ou	CESTMI
	la samedi	CESTMOIWEWE	ou	CESTMO

Seule l'imagination peut limiter les  
 possibilités de l'invention. On peut donner un exemple  
 15 complet de fonctionnement d'un serveur sur des  
 algorithmes convenus avec l'utilisateur.

#### **EXEMPLE DE GESTION DE CES CODES**

20

Dans un exemple de réalisation, illustré  
 sur la figure, à l'achat d'une carte, l'utilisateur choisit,  
 dans un catalogue, l'algorithme qu'il désire et donne  
 les paramètres qui seront utilisés par cet algorithme.

25

Le vendeur saisit le numéro de l'algorithme  
 et les paramètres au nombre maximum de, par exemple,  
 quatre.

Le serveur remplit la table correspondant  
 au fichier de l'utilisateur.

30

Quand l'utilisateur introduit sa carte, les  
 caractéristiques de la carte et du terminal permettent  
 de :

- identifier le porteur de la carte et de  
 trouver son fichier ;

- savoir s'il a accès à l'application et s'il peut l'utiliser actuellement (par exemple code bancaire approvisionné) ;

- connaître sa table de code.

5 L'utilisateur frappe le code correspondant aux paramètres qu'il a lui même définis.

L'utilisateur peut redéfinir les caractéristiques de ce code évolutif, en allant voir la personne qui a accès à l'application. L'utilisateur peut  
10 également changer son algorithme en ligne.

Par exemple les algorithmes choisis et les paramètres à utiliser sont donnés directement en ligne par le responsable de l'introduction de la nouvelle  
15 carte. Il suffit de remplir, dans la table Code\_nom\_de\_l'utilisateur, le code de base, le numéro d'algorithme et les paramètres.

Pour plus de facilités, les algorithmes  
20 peuvent être classés comme suit dans le catalogue :

- algorithmes utilisant l'heure (00 à 11 am/pm ou 00 à 23) ;

- algorithmes utilisant le jour de la semaine (Lu, Ma, ..., Di) ;

25 - algorithmes utilisant la semaine (numéro de la semaine) ;

- algorithmes utilisant le jour du mois (01,...,31) ;

- algorithmes utilisant le mois (numéro du  
30 mois) ;

- algorithmes utilisant l'année (97 ou 1997) ;

- algorithmes utilisant une table particulière ;

- algorithmes utilisant plusieurs paramètres, qui sont la concaténation de plusieurs algorithmes.

5           Quand on parle d'heure, de jour, ..., d'année, il s'agit du contenu du champ correspondant au numéro de l'heure, du jour, ..., de l'année. En fait l'algorithme peut ignorer que ce paramètre est une heure, un jour, ....., une année. Le contenu des tables  
10 indique où il faut prendre la valeur de ce paramètre. Les algorithmes deviennent, dans le serveur :

          - l'algorithme 100 utilise le paramètre 1 ajouté en tête du code de base ;  
          - l'algorithme 101 utilise le paramètre 1  
15 ajouté après le 1er caractère du code de base ;  
          - l'algorithme 102 utilise le paramètre 1 ajouté après le 2ème caractère du code de base ;  
          - l'algorithme 103 utilise le paramètre 1 ajouté après le 3ème caractère du code de base ;  
20           - etc...  
          - l'algorithme 10x utilise le paramètre 1 ajouté à la fin du code de base ;  
          - l'algorithme 200 utilise le paramètre 2 ajouté en tête du code de base ;  
25           - etc...  
          - l'algorithme y0x utilise le paramètre y ajouté à la fin du code de base.

          Pour les exemples 1 et 3 on a l'algorithme 000 : le paramètre est égal à i ; on enlève le ième  
30 caractère.

          La Table\_Code\_nom\_de\_l'utilisateur permet de retrouver le contenu du paramètre. Elle a la forme suivante :

35

	Code de base	Code de base	Code de secours
	Algorithmes	Algorithme de base	Algorithme de secours
5	Paramètre 1	Type	Table
	Paramètre 2	Type	Table
	Paramètre n	Type	Table

10 où Type=l'heure, le jour, la semaine, le mois, l'année  
ou la table définie dans Table.

On donne ici la possibilité d'utiliser un  
code et un algorithme de secours. Cela permet de varier  
les possibilités mais complique la gestion des tables.  
15 Le choix du code peut être fait en ligne.

Dans le premier exemple :

20 • Vu par l'utilisateur

Il est 14 heures et on est en novembre, son  
code personnel (de base) est JPM. Il tape J14P11M.

• Vu par le serveur

25 La carte introduite dans le publiphone  
78456 indique au serveur que Monsieur Jean-Pierre  
Mounier veut accéder à un service de France Telecom qui  
exige un code sécurisé.

30 Dans le fichier Jean\_Pierre\_Mounier il y a  
la table : Code\_Jean\_Pierre\_Mounier :

	Code de base	JPM	Pas de code de secours
	Algorithmes	101-102	Pas d'algorithme de secours
	Paramètre 1	Type = heure	
35	Paramètre 2	Type = mois	
		FIN	



L'algorithme à utiliser est 101-202 (deux paramètres).

Algorithme 101 :

5 Ajouter P1 en Code\_de\_base [caractère\_1+1]  
commentaires : car1, P1, car2, car3, ..., carn

Algorithme 202 :

Ajouter P2 en Code\_de\_base [caractère\_2+1]  
commentaire : car1, P1, car2, P2, car3, ..., carn

10

Code\_de\_base = JPM

P1 = l'heure = 14

P2 = le mois = 11

15 Code attendu = J14P11M, c'est bien celui qui a été  
frappé.

Dans le second exemple :

20 • Vu par l'utilisateur

On est vendredi, le semaine est finie, le  
code de base est CESTMOI. Je tape CESTMOIFINI.

• Vu par le serveur

25 La table Code\_Jean\_Pierre\_Mounier a la  
forme suivante :

30	Code de base	JPM	Pas de code de secours
	Algorithmes	109	Pas d'algorithme de secours
	Paramètre 1	Type = jour de semaine	Table = JPM1
		FIN	

35 L'algorithme 109 utilise le paramètre 1  
ajouté à la fin du code de base.

La table JPM1 a la forme suivante :

	Dimanche	REPOS
	Lundi	DEBUT
5	Mardi	MARS
	Mercredi	ECOL
	Jeudi	JEUD
	Vendredi	FINI
10	Samedi	WEWE

On est le 6 juin 1997, c'est un vendredi.  
 La table JPM1 donne FINI pour vendredi. Le code de base  
 est CESTMOI. L'algorithme 109 dit d'ajouter le contenu  
 de la table JPM1 au code de base. Le code attendu est  
 15 CESTMOIFINI.

Dans le troisième exemple :

20 • Vu par l'utilisateur

Cette méthode demande plus de réflexion de  
 la part de l'utilisateur. On est le lundi 9 juin. C'est un  
 lundi deuxième jour de la semaine. Donc l'utilisateur doit  
 enlever la deuxième lettre de son code qui est CESTMOI.  
 25 Donc il enlève le E et il obtient CSTMOI.

On voit ici que l'utilisateur a intérêt à  
 utiliser un algorithme intuitif et simple.

• Vu par le serveur

30 La table Code\_Jean\_Pierre\_Mounier a la  
 forme suivante :

	Code de base	JPM	Pas de code de secours
	Algorithmes	000	Pas d'algorithme de secours
35	Paramètre 1	Type = jour	JPM1

	de semaine	
	FIN	

La table JPM1 a la forme suivante :

5

Dimanche	1
Lundi	2
Mardi	3
Mercredi	4
Jeudi	5
Vendredi	6
Samedi	7

10

15

On est le 9 juin 1997, c'est un lundi. La table JPM1 donne 2 pour lundi. Le code de base est CESTMOI. L'algorithme 000 dit d'enlever le ième caractère au code de base. Ici i est égal à 2. Le code attendu est CESTMOI moins la deuxième lettre, c'est-à-dire CSTMOI.

20

On peut aller du plus simple : l'utilisateur donne le jour de la semaine, au plus compliqué du style : le code de base est Jean-Pierre Mounier, l'utilisateur le transforme en :

25

1. Il enlève la lettre correspondant au jour de la semaine.
2. Il ajoute le numéro de la semaine après Jean.
3. Il ajoute le numéro du mois après Pierre.
4. Il ajoute en fin de code l'heure.

30

Ce qui donne : on est le 9 juin à 15h30 et c'est un lundi :

35

1. Il enlève la lettre correspondant au  
jour de la semaine (2) ⇒  
JanPierreMounier.
2. Il ajoute le numéro de la semaine après  
5 Jean (24) ⇒ Jan24PierreMounier.
3. Il ajoute le numéro du mois après Pierre  
(06) ⇒ Jan24Pierre06Mounier.
4. Il ajoute en fin de code l'heure (15) ⇒  
10 Jan24Pierre06Mounier15.

Ce code est inutilisable pour un tiers et le serveur  
s'y retrouve facilement.

REVENDEICATIONS

1. Procédé d'accès à une application  
comprenant une étape de mise en place, par le  
5 responsable de cette application, d'un code d'accès à  
celle-ci, et une étape d'introduction, par un usager  
d'un système informatique, de ce code permettant à  
celui-ci d'utiliser cette application, caractérisé en  
ce que dans la première étape le responsable de  
10 l'application choisit une modification automatique du  
code suivant un algorithme d'évolution en partant d'un  
code de base.

2. Procédé selon la revendication 1, dans  
lequel on a les étapes suivantes :

15 - à l'achat d'une carte, l'usager  
choisit, dans un catalogue, l'algorithme qu'il désire  
et donne les paramètres qui seront utilisés par cet  
algorithme ; le vendeur de la carte saisit le numéro de  
l'algorithme et les paramètres ; un serveur remplit la  
20 table correspondant au fichier de l'usager ;

- quand l'usager introduit sa carte les  
caractéristiques de la carte et du terminal permettent  
de :

25 . identifier le porteur de la carte  
et de trouver son fichier,  
. savoir s'il a accès à l'application  
et s'il peut l'utiliser  
actuellement,  
. connaître sa table de code ;  
30 - l'usager frappe le code correspondant  
aux paramètres qu'il a lui-même définis.

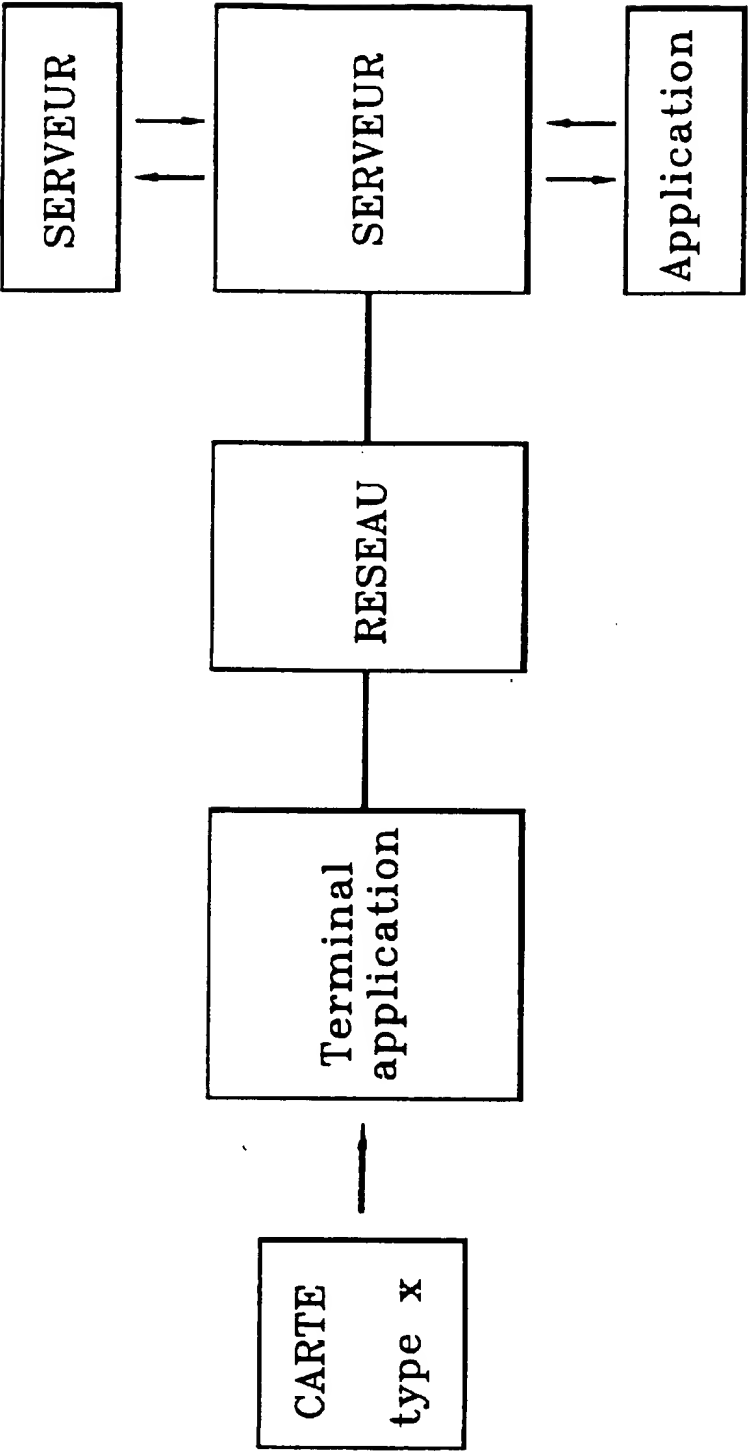
3. Procédé selon la revendication 1,  
caractérisé l'algorithme est pris parmi les algorithmes  
suivants :

35 - algorithmes utilisant l'heure ;

- semaine ;
  - algorithmes utilisant le jour de la
- 5 mois ;
  - algorithmes utilisant la semaine ;
  - algorithmes utilisant le jour du
- particulière ;
  - algorithmes utilisant le mois ;
  - algorithmes utilisant l'année ;
  - algorithmes utilisant une table
- 10
  - algorithmes utilisant plusieurs paramètres, qui sont la concaténation de plusieurs algorithmes.
- 15
  - 4. Procédé selon la revendication 1, dans lequel on utilise un algorithme de secours.
  - 5. Procédé selon la revendication 1, dans lequel le choix de l'algorithme est fait en ligne.

1/1

FIG. 1



RAPPORT DE RECHERCHE  
PRELIMINAIREétabli sur la base des dernières revendications  
déposées avant le commencement de la recherche

2770067

N° d'enregistrement  
nationalFA 551482  
FR 9712973

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
Y	EP 0 561 685 A (FUJITSU LTD) 22 septembre 1993 * abrégé; figures 1,2 * * colonne 3, ligne 32 - colonne 4, ligne 46 * ---	1,2,5
Y	US 5 163 097 A (PEGG TINA C) 10 novembre 1992 * le document en entier * ---	1,2,5
A	WO 87 03977 A (GORDIAN SYSTEMS INC) 2 juillet 1987 * le document en entier * ---	1,3
A	US 5 509 070 A (SCHULL JONATHAN) 16 avril 1996 * le document en entier * ---	1,3
A	WO 96 34328 A (WEISZ HERMAN ; LO PIANO ORNELLA (IT)) 31 octobre 1996 * abrégé * ---	1,3
A	WO 97 36221 A (ROLM SYSTEMS) 2 octobre 1997 * page 2, alinéa 2 - page 3, alinéa 1 * -----	1,4
		DOMAINES TECHNIQUES RECHERCHES (Int.C.L.6)
		G06F
Date d'achèvement de la recherche		Examineur
10 juillet 1998		Powell, D
CATEGORIE DES DOCUMENTS CITES		
X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général O : divulgation non-écrite P : document intercalaire T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant		



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**